95 – Janeiro 2008

PCI e o Real Valor do Compliance – parte 1

Há quase dez anos publico opiniões relacionadas à gestão de riscos, continuidade de negócios, governança e inteligência competitiva, e desde então, me vejo às voltas com novas normas, padrões e conseqüentemente, com o esforço do mercado em identificar os impactos diretos e indiretos de cada um deles em seus negócios, bem como em tangibilizar os valores que adicionam e convertê-los em resultado.

O mais recente alvo do compliance tem sido o mercado financeiro de pagamentos, mais especificamente de cartões de crédito, através do PCI DSS ou *Payment Card Industry Data Security Standard*. Não é por menos. Há décadas se vê o crescimento do dinheiro de plástico até se tornar uma das principais formas de pagamento nos mais fortes mercados mundiais. Falando especificamente de Brasil e transações via Internet, dados da Câmara Brasileira de Comércio Eletrônico mostram que a aquisição de bens de consumo, veículos e serviços ligados ao turismo movimentou R$ 4,4 bilhões no primeiro trimestre deste ano. O número representa um avanço de 57% em relação ao mesmo período no ano passado. Ao todo são mais de 5,7 milhões de consumidores virtuais, cujo *ticket* médio fica em torno de 380 reais.

Acompanhando este ritmo de crescimento, vêm os indicadores de fraude. De acordo com os organismos internacionais, o custo das fraudes com cartão de crédito ultrapassa os bilhões de dólares anualmente, sendo que em 2007, só no Reino Unido, o volume foi estimado em 800 milhões de dólares, indicando uma média de crescimento de 350%. No Brasil, de acordo com os dados da FEBRABAN, os prejuízos somaram mais de 150 milhões de dólares em fraudes praticadas apenas em meios de pagamento eletrônico no mesmo ano.

Diante de números tão alarmantes, julguei conveniente escrever desta vez sobre a importância do PCI, sua história, suas implicações e assim, ajudar as empresas, mesmo que introdutoriamente, a compreender o valor do compliance e a conhecer os melhores caminhos para alcançá-lo, aproveitando as experiências que venho colecionando no mercado Europeu desde 2005.

O que é o PCI DSS?

Payment Card Industry Data Security Standard é um padrão de segurança para proteção de dados de cartão de crédito introduzido em 2001 pela VISA dos Estados Unidos. O principal objetivo do padrão foi reduzir as fraudes em larga escala com cartão de crédito em ambientes de pagamento eletrônico, tanto via Internet quanto em estabelecimentos comerciais tradicionais. O DSS é dividido em seis principais áreas, que por sua vez, se desdobram em doze requerimentos. O documento contém padrões de segurança que cobrem os seguintes temas: segregação e segurança de redes; criptografia para proteção de dados de cartão; gerenciamento de atualizações e auditoria de vulnerabilidades em sistemas; medidas de controle de acesso e integridade de arquivos; teste e monitoramento de redes, e ainda gestão de incidentes e manutenção da política de segurança da informação.

Como surgiu?

Em 2001 a Mastercard introduziu seu programa chamado *Site Data Protection* que define a necessidade de uma varredura externa periódica de vulnerabilidades, além de definir padrões para *patching* de sistemas; segurança de bancos de dados e *firewall* de rede. Finalmente em 2004 a Visa somou esforços com a Mastercard para consolidar o PCI DSS. Em 2006 o controle sobre o programa de conformidade PCI, foi transferido para uma nova organização chamada *PCI Security Council*, acessível pelo endereço eletrônico *www.pcisecuritystandards.org*, onde é possível encontrar todo tipo de documentação de suporte.

Quem precisa estar em conformidade?

O PCI DSS se aplica a toda e qualquer empresa que coleta, processa, armazena ou transmite informação de cartão de crédito, estando, portanto, obrigada a aderir e se tornar *compliant* com o padrão. Em linhas gerais, nesta lista incluem-se os comerciantes, intermediários que processam dados de cartão de crédito e estão ligados à rede da associação de cartões, assim como provedores de serviço que hospedam website, processam transações em ATM ou coletam e processam dados de cartão de crédito em nome de membros das redes Visa e Mastercard, ou seja, que agem como *gateways* de pagamento. A exceção fica com empresas que apenas emitem cartões de crédito e autorizam transações, como bancos e grandes varejistas, deixando de ser obrigados a demonstrar conformidade com o PCI DSS.
Em contrapartida, assim como vem ocorrendo com a norma de gestão de segurança da informação BS7799, ISO 17799 ou mais recentemente, ISO27001, muitas empresas que estão fora do radar oficial de *compliance* vêm valor em se alinhar à norma com o objetivo de tornar a operação de seus negócios mais robusta, confiável e assim, fortalecer sua reputação. Empresas fabricantes de softwares comerciais que, de alguma forma, intermediam ou planejam intermediar processos de pagamento, por exemplo, começam a desenvolver programas e procurar auxílio externo para tornar seus produtos prontos para o PCI através da PABP ou *Payment Application Best Practice*. Não buscam o compliance, por não ser aplicável, mas adotam muitas das recomendações da norma para que seus produtos possam se integrar futuramente à perímetros PCI ou à cadeia produtiva de empresas que precisam ter e manter a conformidade com o PCI.

Qual o prazo e o nível de aderência atual?

O cronograma de conformidade varia de acordo com o continente e o mercado. No Brasil as empresas físicas e virtuais que estão dentro do escopo do PCI terão até 2009 para se adequarem. Entretanto, o resultado de uma pesquisa feita em 2006 no mercado norte americano revelou que menos de 20% de todos os grandes varejistas e provedores de serviço atingiram a conformidade plena com o PCI DSS. Já em 2007, a mesma pesquisa chegou ao índice de 35% de conformidade. Para todos os demais que ainda estão buscando a conformidade, é preciso documentar detalhadamente seus programas de compliance e planos de ação que irão mitigar os riscos e levá-los à conformidade.

Considerando a heterogeneidade dos ambientes operacionais e dos modelos de negócio das empresas envolvidas no *compliance*, podem surgir dificuldades em implementar alguns dos requerimentos. Nesses casos, será preciso definir e implementar controles compensatórios de forma a alcançar o nível de risco residual adequado.

A segunda e última parte deste artigo irá tratar dos impactos da não conformidade, os responsáveis pelo programa, o rigor das avaliações de segurança e ainda, como começar um planejamento de aderência ao PCI. Aguarde.

Marcos Sêmola *é IT Compliance Manager da Shell International Limited Gas & Power na Holanda, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação, governança e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br*

Nota: Este artigo expressa exclusivamente a opinião pessoal do autor, não representando necessariamente a opinião da empresa citada.